

1 **KOPELOWITZ OSTROW PA**
2 Kristen Lake Cardoso (State Bar No. 338762)
3 1 West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Email: cardoso@kolawyers.com

4

5 *Attorneys for Plaintiff*

6

7 **IN THE UNITED STATES DISTRICT COURT**
FOR THE CENTRAL DISTRICT OF CALIFORNIA

8

9 PATRICIA LOPEZ, individually
10 and on behalf of all others similarly
situated,

11 Plaintiff,

12 v.

13 CITY OF HOPE NATIONAL
MEDICAL CENTER,

14 Defendant.

15 Case No.: _____

16

17 **PLAINTIFF'S CLASS ACTION
COMPLAINT FOR:**

1. NEGLIGENCE
2. NEGLIGENCE PER SE;
3. BREACH OF IMPLIED
CONTRACT;
4. BREACH OF FIDUCIARY
DUTY;
5. BREACH OF CONFIDENCE;
6. UNJUST ENRICHMENT; and
7. INJUNCTIVE/DECLARATORY
RELIEF

18

19 **DEMAND FOR JURY TRIAL**

20 Plaintiff, Patricia Lopez ("Plaintiff"), individually and on behalf of a class of
similarly situated persons, brings this Class Action Complaint and alleges the
following against Defendant, City of Hope National Medical Center ("City of Hope"
or "Defendant"), based upon personal knowledge with respect to Plaintiff and on
information and belief derived from, among other things, investigation of counsel
and review of public documents as to all other matters.

21

22 **INTRODUCTION**

23

24 1. Data Breaches have become entirely too common, and the reason is the
lack of attention and resources that companies like Defendant expend on protecting
sensitive information.

25

26 2. Plaintiff brings this class action against City of Hope for its failure to
properly secure Plaintiff's and Class Members' personally identifiable information

1 (“PII”) and personal health information (“PHI”) (together, “Private Information”).
2 According to City of Hope, the Private Information may have included patients’
3 names, addresses, phone numbers, dates of birth, Social Security numbers, health
4 insurance information, medical records, information about medical history and/or
5 associated conditions, and/or unique identifiers to associate individuals with City of
6 Hope.¹

7 3. City of Hope failed to comply with industry standards to protect
8 information systems that contain Private Information. Plaintiff seeks, among other
9 things, orders requiring City of Hope to fully and accurately disclose the nature of
10 the information that has been compromised and to adopt sufficient security practices
11 and safeguards to prevent incidents like the disclosure (the “Data Breach”) in the
12 future.

13 4. The Private Information compromised in the Data Breach included
14 personal identifiable information of individuals whose Private Information was
15 maintained by Defendant, including Plaintiff.

16 5. The Data Breach was a direct result of Defendant’s failure to implement
17 adequate and reasonable cyber-security procedures and protocols necessary to
18 protect individuals’ Private Information with which it was hired to protect.

19 6. Upon information and belief, the mechanism of the Data Breach and
20 potential for improper disclosure of Plaintiff’s and Class Members’ Private
21 Information was a known risk to Defendant, and thus Defendant was on notice that
22 failing to take steps necessary to secure Private Information from those risks left that
23 property in a dangerous condition.

24 7. Upon information and belief, Defendant breached its duties and
25 obligations by failing, in one or more of the following ways: (1) failing to design,
26 implement, monitor, and maintain reasonable network safeguards against

28 1 Notice of Security Incident, City of Hope, <https://www.cityofhope.org/notice-of-data-security-incident> (last visited April 8, 2024).

1 foreseeable threats; (2) failing to design, implement, and maintain reasonable data
2 retention policies; (3) failing to adequately train staff on data security; (4) failing to
3 comply with industry-standard data security practices; (5) failing to warn Plaintiff
4 and Class Members of Defendant's inadequate data security practices; (6) failing to
5 encrypt or adequately encrypt the Private Information; (7) failing to recognize or
6 detect that its network had been compromised and accessed in a timely manner to
7 mitigate the harm; (8) failing to utilize widely available software able to detect and
8 prevent this type of attack, and (9) otherwise failing to secure the hardware using
9 reasonable and effective data security procedures free of foreseeable vulnerabilities
10 and data security incidents.

11 8. Defendant disregarded the rights of Plaintiff and Class Members
12 (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently
13 failing to take adequate and reasonable measures to ensure its data systems were
14 protected against unauthorized intrusions; failing to disclose that it did not have
15 adequately robust computer systems and security practices to safeguard Plaintiff's
16 and Class Members' Private Information; failing to take standard and reasonably
17 available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and
18 Class Members with prompt and full notice of the Data Breach.

19 9. In addition, Defendant failed to properly maintain and monitor the
20 computer network and systems that housed the Private Information. Had it properly
21 monitored its property, it would have discovered the intrusion sooner rather than
22 allowing cybercriminals a period of unimpeded access to the Private Information of
23 Plaintiff and Class Members.

24 10. Plaintiff's and Class Members' identities are now at risk because of
25 Defendant's negligent conduct since the Private Information that Defendant
26 collected and maintained is now in the hands of data thieves.

27 11. As a result of the Data Breach, Plaintiff and Class Members are now at
28 a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class

1 Members must now and for years into the future closely monitor their financial
2 accounts to guard against identity theft. As a result of Defendant's unreasonable and
3 inadequate data security practices, Plaintiff and Class Members have suffered
4 numerous actual and concrete injuries and damages.

5 12. The risk of identity theft is not speculative or hypothetical but is
6 impending and has materialized as there is evidence that the Plaintiff's and Class
7 Members' Private Information was targeted, accessed, has been misused, and
8 disseminated on the Dark Web.

9 13. Plaintiff and Class Members must now closely monitor their financial
10 accounts to guard against future identity theft and fraud. Plaintiff and Class Members
11 have heeded such warnings to mitigate against the imminent risk of future identity
12 theft and financial loss. Such mitigation efforts included and will continue to include
13 in the future, among other things: (a) reviewing financial statements; (b) changing
14 passwords; and (c) signing up for credit and identity theft monitoring services. The
15 loss of time and other mitigation costs are tied directly to guarding against the
16 imminent risk of identity theft.

17 14. Plaintiff and Class Members have suffered numerous actual and
18 concrete injuries as a direct result of the Data Breach, including: (a) financial costs
19 incurred mitigating the materialized risk and imminent threat of identity theft; (b)
20 loss of time and loss of productivity incurred mitigating the materialized risk and
21 imminent threat of identity theft; (c) financial costs incurred due to actual identity
22 theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value
23 of their Private Information; and (h) the continued risk to their sensitive Private
24 Information, which remains in the possession of Defendant, and which is subject to
25 further breaches, so long as Defendant fails to undertake appropriate and adequate
26 measures to protect it collected and maintained.

27 15. Through this Complaint, Plaintiff seeks to remedy these harms on
28 behalf of herself and all similarly situated individuals whose Private Information

1 | was accessed during the Data Breach.

2 16. Accordingly, Plaintiff brings this action against Defendant seeking
3 redress for its unlawful conduct and asserting claims for: (i) negligence and
4 negligence *per se*, (ii) breach of implied contract, (iii) breach of fiduciary duty (iv)
5 unjust enrichment.

6 17. Plaintiff seeks remedies including, but not limited to, compensatory
7 damages, reimbursement of out-of-pocket costs, and injunctive relief including
8 improvements to Defendant's data security systems, future annual audits, as well as
9 long-term and adequate credit monitoring services funded by Defendant, and
10 declaratory relief.

11 18. The exposure of one's Private Information to cybercriminals is a bell
12 that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private
13 Information was exactly that—private. Not anymore. Now, their Private Information
14 is forever exposed and unsecure.

PARTIES

16 19. Plaintiff is an adult individual who at all relevant times has been a
17 citizen and resident of California, who has been a patient at City of Hope in recent
18 years. She gave Private Information to City of Hope as a condition of receiving
19 medical services.

20 20. Defendant is a Nonprofit Corporation formed in California, with its
21 principal place of business at 1500 E Duarte Rd, Duarte, California 91010.

21. Upon information and belief, at the time of the Data Breach, Defendant
22 retained Plaintiff's Private Information in its system.
23

24 22. Plaintiff is very careful about sharing her sensitive Private Information.
25 Plaintiff stores any documents containing her Private Information in a safe and
26 secure location. She has never knowingly transmitted unencrypted sensitive Private
27 Information over the internet or any other unsecured source.

1 23. Plaintiff is not aware of ever being part of a data breach involving her
2 Private Information and is concerned that it and other private information has now
3 been exposed to bad actors. As a result, she has taken multiple steps to avoid identity
4 theft, including closing her accounts, checking her credit monitoring service, setting
5 up notices and reports and carefully reviewing all her accounts.

6 24. As a result of the Data Breach, Plaintiff made reasonable efforts to
7 mitigate the impact of the Data Breach, including but not limited to researching the
8 Data Breach, and reviewing credit reports and financial account statements for any
9 indications of actual or attempted identity theft or fraud. Plaintiff has already spent
10 multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would
11 have spent on other activities.

12 25. Plaintiff suffered actual injury from having her Private Information
13 compromised as a result of the Data Breach including, but not limited to (a) damage
14 to and diminution in the value of Private Information, a form of property that
15 Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present,
16 imminent and impending injury arising from the increased risk of identity theft and
17 fraud.

18 26. Plaintiff anticipates spending considerable time and money on an
19 ongoing basis to try to mitigate and address harms caused by the Data Breach. As a
20 result of the Data Breach, Plaintiff is at a present risk and will continue to be at
21 increased risk of identity theft and fraud for years to come.

JURISDICTION AND VENUE

23 27. This Court has subject matter jurisdiction over this action under the
24 Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy
25 exceeds \$5 million, exclusive of interest and costs. The number of class members
26 exceeds 100, some of whom have different citizenship from Defendant. Thus,
27 minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

28. This Court has personal jurisdiction over Defendant because it is a California corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

29. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

The Data Breach

1. On October 13, 2023, Defendant became aware of suspicious activity on a “subset of its systems”².

2. City of Hope's disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why Private Information were stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what City of Hope knows about the degree to which the data has been disseminated.

3. City of Hope has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, City of Hope has taken to secure the Private Information still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff and Class Members' interests, and ensure that City of Hope has proper measures in place to prevent similar incidents from occurring in the future.

² Notice of Security Incident, City of Hope, <https://www.cityofhope.org/notice-of-data-security-incident> (last visited April 8, 2024).

1 **The Healthcare Sector is a Primary Target for Data Breaches**

2 4. City of Hope was on notice that companies in the healthcare industry
 3 are susceptible targets for data breaches.

4 5. City of Hope was also on notice that the Federal Bureau of Investigation
 5 has been concerned about data security in the healthcare industry. On April 8, 2014,
 6 the FBI's Cyber Division issued a Private Industry Notification to companies within
 7 the healthcare sector, stating that "the health care industry is not technically prepared
 8 to combat against cyber criminals' basic cyber intrusion tactics, techniques and
 9 procedures (TTPs), much less against more advanced persistent threats (APTs)" and
 10 pointed out that "[t]he biggest vulnerability was the perception of IT healthcare
 11 professionals' beliefs that their current perimeter defenses and compliance strategies
 12 were working when clearly the data states otherwise." The same warning specifically
 13 noted that "[t]he FBI has observed malicious actors targeting healthcare-related
 14 systems, perhaps for the purpose of obtaining Protected Health Information (PHI)
 15 and/or PII."³

16 6. The number of reported North American data breaches increased by
 17 over 50 percent in 2021, from 1,080 in 2020⁴, to 1,638 in 2021.⁵ As a recent report
 18 reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking
 19 attacks and the more impactful ransomware campaigns."⁶

20 7. At the end of 2018, the healthcare sector ranked second in the number
 21 of data breaches among measured sectors, and had the highest rate of exposure for

22 ³ Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions
 23 for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry
 24 Notification (available at <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf>) (last accessed Mar. 14, 2023).

25 ⁴ See Verizon 2021 Data Breach Investigations Report, at 97,
<https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf> (last accessed Mar. 14, 2023).

26 ⁵ See Verizon 2022 Data Breach Investigations Report, at 83 (available at
<https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>) (last accessed Mar. 14, 2023).

27 ⁶ *Id.* at 62.

1 each breach.⁷ Indeed, when compromised, healthcare related data is among the most
 2 sensitive and personally consequential. A report focusing on healthcare breaches
 3 found that the “average total cost to resolve an identity theft-related incident . . .
 4 came to about \$20,000,” and that the victims were often forced to pay out-of-pocket
 5 costs for healthcare they did not receive in order to restore coverage.⁸ Almost 50
 6 percent of the victims lost their healthcare coverage as a result of the incident, while
 7 nearly 30 percent said their insurance premiums went up after the event. Forty
 8 percent of the customers were never able to resolve their identity theft at all. Data
 9 breaches and identity theft have a crippling effect on individuals and detrimentally
 10 impact the economy.⁹

11 8. Healthcare-related breaches have persisted because criminals see
 12 electronic patient data as a valuable asset. According to the 2019 HIMSS
 13 Cybersecurity Survey, 82 percent of participating hospital information security
 14 leaders reported having a significant security incident in the previous 12 months,
 15 with a majority of these known incidents being caused by “bad actors” such as
 16 cybercriminals.¹⁰ “Hospitals have emerged as a primary target because they sit on a
 17 gold mine of sensitive personally identifiable information for thousands of patients
 18 at any given time. From social security and insurance policies, to next of kin and
 19 credit cards, no other organization, including credit bureaus, have so much
 20 monetizable information stored in their data centers.”¹¹

21 7 *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center (available
 22 at <https://www.idtheftcenter.org/2018-data-breaches>) (last accessed Mar. 14,
 23 2023).

24 8 Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3,
 25 2010) (available at <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>) (last accessed Mar. 14, 2023).

26 9 *Id.*

27 10 *2019 HIMSS Cybersecurity Survey* (available at
 28 https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Mar. 14, 2023).

29 11 Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing
 Attacks*, Apr. 4, 2019 (available at <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks>) (last accessed Mar. 14, 2023).

1 9. The American Medical Association (“AMA”) has also warned
2 healthcare companies about the importance of protecting their patients’ confidential
3 information:

4 Cybersecurity is not just a technical issue; it’s a patient safety
5 issue. AMA research has revealed that 83% of physicians
6 work in a practice that has experienced some kind of
7 cyberattack. Unfortunately, practices are learning that
8 cyberattacks not only threaten the privacy and security of
9 patients’ health and financial information, but also patient
10 access to care.¹²

11 10. As a major healthcare provider, City of Hope knew, or should have
12 known, the importance of safeguarding the patients’ Private Information entrusted
13 to it and of the foreseeable consequences if that data was disclosed. This includes
14 the significant costs that would be imposed on City of Hope patients because of a
15 breach. City of Hope failed, however, to take adequate cybersecurity measures to
16 prevent the Data Breach.

17 **City of Hope Stores Plaintiff and Class Members’ Private Information**

18 11. City of Hope obtains and stores a massive amount of its patients’
19 Private Information. As a condition of engaging in health services, City of Hope
20 requires that patients entrust it with highly confidential Private Information.

21 12. By obtaining, collecting, using, and deriving a benefit from Plaintiff
22 and Class Members’ Private Information, City of Hope assumed legal and equitable
23 duties and knew or should have known that it was responsible for protecting Plaintiff
24 and Class Members’ Private Information from disclosure.

25 13. Plaintiff and Class Members have taken reasonable steps to maintain
26 the confidentiality of their Private Information and, as City of Hope’s current and
27 former patients, they rely on City of Hope to keep this information confidential and
28 securely maintained, and to make only authorized disclosures of this information.

29 ¹² Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics,*
30 *hospitals*, Am. Med. Ass’n (Oct. 4, 2019) (available at <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals>) (last visited Mar. 14, 2023).

1 **Private Information are Valuable and Subject to Unauthorized Disclosure**

2 14. City of Hope was aware that the Private Information it collects is highly
 3 sensitive and of significant value to those who would use it for wrongful purposes.

4 15. Private Information are valuable commodities to identity thieves. As
 5 the FTC recognizes, identity thieves can use this information to commit an array of
 6 crimes including identify theft, and medical and financial fraud.¹³ Indeed, a robust
 7 illegal market exists in which criminals openly post stolen Private Information on
 8 multiple underground websites, commonly referred to as the “dark web.” PHI can
 9 sell for as much as \$363 on the dark web, according to the Infosec Institute.¹⁴

10 16. PHI is particularly valuable because criminals can use it to target
 11 victims with frauds and swindles that take advantage of the victim’s medical
 12 conditions or victim settlements. It can be used to create fake insurance claims,
 13 allowing for the purchase and resale of medical equipment, or gain access to
 14 prescriptions for illegal use or resale.

15 17. Medical identify theft can result in inaccuracies in medical records and
 16 costly false claims. It can also have life-threatening consequences. If a victim’s PHI
 17 is mixed with other records, it can lead to misdiagnosis or mistreatment. “Medical
 18 identity theft is a growing and dangerous crime that leaves its victims with little to
 19 no recourse for recovery,” reported Pam Dixon, executive director of World Privacy
 20 Forum. “Victims often experience financial repercussions and worse yet, they
 21 frequently discover erroneous information has been added to their personal medical
 22 files due to the thief’s activities.”¹⁵

23
 24 ¹³ Federal Trade Commission, What To Know About Identity Theft (available at
 25 <https://consumer.ftc.gov/articles/what-know-about-identity-theft>) (last accessed
 26 Mar. 14, 2023).

27 ¹⁴ Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available
 28 at <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/>) (last
 accessed Mar. 14, 2023).

29 ¹⁵ Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health
 30 News (Feb. 7, 2014) (available at <https://khn.org/news/rise-of-indentity-theft/>) (last
 31 accessed Mar. 14, 2023).

18. The ramifications of City of Hope's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

19. Further, criminals often trade stolen Private Information for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

20. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.¹⁶ This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.¹⁷

21. City of Hope knew, or should have known, the importance of safeguarding its patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on City of Hope patients because of a breach. City of Hope failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

22. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of their rights. They are

¹⁶ See Medical ID Theft Checklist (available at <https://www.identityforce.com/blog/medical-id-theft-checklist-2>) (last accessed Mar. 14, 2023).

¹⁷ Experian, The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches (available at <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>) (last accessed Mar. 14, 2023).

1 incurring and will continue to incur such damages in addition to any fraudulent use
2 of their Private Information.

3 23. Despite all the publicly available knowledge of known and foreseeable
4 consequences of the disclosure of Private Information, City of Hope's policies and
5 practices with respect to maintaining the security of its patients' Private Information
6 were reckless, or at the very least, negligent.

7 24. In virtually all contexts, the expenditure of time has consistently been
8 recognized as compensable, and for many people, it is the basis on which they are
9 compensated. Plaintiff and Class Members should be compensated for the time they
10 have expended because of City of Hope's misfeasance.

11 25. Once Private Information are stolen, fraudulent use of that information
12 and damage to victims may continue for years. Consumer victims of data breaches
13 are more likely to become victims of identity fraud.¹⁸

14 26. As a result of the wide variety of injuries that can be traced to the Data
15 Breach, Plaintiff and Class Members have and will continue to suffer financial loss
16 and other actual harm for which they are entitled to damages, including, but not
17 limited to, the following:

- 18 a. losing the inherent value of their Private Information;
- 19 b. identity theft and fraud resulting from the theft of their Private
20 Information;
- 21 c. costs associated with the detection and prevention of identity theft;
- 22 d. costs associated with purchasing credit monitoring, credit freezes, and
23 identity theft protection services;
- 24 e. lowered credit scores resulting from credit inquiries following
25 fraudulent activities;

26
27 ¹⁸ 2014 LexisNexis True Cost of Fraud Study (available at
28 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>) (last
 accessed Mar. 14, 2023).

- 1 f. costs associated with time spent and the loss of productivity or the
2 enjoyment of one's life from taking time to address and attempt to
3 mitigate and address the actual and future consequences of the Data
4 Breach, including discovering fraudulent charges, cancelling and
5 reissuing cards, purchasing credit monitoring and identity theft
protection services, imposing withdrawal and purchase limits on
6 compromised accounts, and the stress, nuisance, and annoyance of
7 dealing with the repercussions of the Data Breach; and
8 g. the continued imminent injury flowing from potential fraud and
identify theft posed by their Private Information being in the possession
9 of one or more unauthorized third parties.

City of Hope's Lax Security Violates HIPAA

13 27. City of Hope had a non-delegable duty to ensure that all PHI it collected
14 and stored was secure.

15 28. City of Hope is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a
16 result, is required to comply with the HIPAA Privacy Rule and Security Rule, 45
17 C.F.R Part 160 and Part 164, Subparts A and E (“Standards for Privacy of
18 Individually Identifiable Health Information”), and Security Rule (“Security
19 Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R.
20 Part 160 and Part 164, Subparts A and C.

21 29. These rules establish national standards for the protection of patient
22 information, including protected health information, defined as “individually
23 identifiable health information” which either “identifies the individual” or where
24 there is a “reasonable basis to believe the information can be used to identify the
25 individual,” that is held or transmitted by a healthcare provider. See 45 C.F.R. §
26 160.103.

27 30. HIPAA limits the permissible uses of “protected health information”
28 and prohibits unauthorized disclosures of “protected health information.”

1 31. HIPAA requires that City of Hope implement appropriate safeguards
2 for this information.

3 32. Despite these requirements, City of Hope failed to comply with its
4 duties under HIPAA and its own Privacy Practices. In particular, City of Hope failed
5 to:

- 6 a. maintain an adequate data security system to reduce the risk of data
7 breaches and cyber-attacks;
- 8 b. adequately protect Plaintiff and Class Members' PHI;
- 9 c. ensure the confidentiality and integrity of electronic PHI created,
10 received, maintained, or transmitted, in violation of 45 C.F.R. §
11 164.306(a)(1);
- 12 d. implement technical policies and procedures for electronic
13 information systems that maintain electronic PHI to allow access only
14 to those persons or software programs that have been granted access
15 rights, in violation of 45 C.F.R. § 164.312(a)(1);
- 16 e. implement adequate policies and procedures to prevent, detect,
17 contain, and correct security violations, in violation of 45 C.F.R. §
18 164.308(a)(1)(i);
- 19 f. implement adequate procedures to review records of information
20 system activity regularly, such as audit logs, access reports, and
21 security incident tracking reports, in violation of 45 C.F.R. §
22 164.308(a)(1)(ii)(D);
- 23 g. protect against reasonably anticipated uses or disclosures of electronic
24 PHI that are not permitted under the privacy rules regarding
25 individually identifiable health information, in violation of 45 C.F.R.
26 § 164.306(a)(3);
- 27 h. ensure compliance with the electronic PHI security standard rules by
28 its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

- i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b)

33. City of Hope failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff and Class Members' PHI.

City of Hope Violated FTC Guidelines

34. The Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45, prohibited City of Hope from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ PII is an “unfair practice” in violation of the FTC Act. *See, e.g., Fed. Trade Comm’n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

35. The FTC has promulgated several guides for businesses that reflect the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.¹⁹

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.²⁰ The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

¹⁹ Federal Trade Commission, Start With Security: A Guide for Business (available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>) (last accessed Mar. 14, 2023).

²⁰ Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Mar. 14, 2023).

1 37. The FTC further recommends that companies not maintain PII longer
2 than is needed for authorization of a transaction; limit access to confidential data;
3 require complex passwords to be used on networks; use industry-tested methods for
4 security; monitor for suspicious activity on the network; and verify that third-party
5 service providers have implemented reasonable security measures.²¹

6 38. The FTC has brought enforcement actions against businesses for failing
7 to protect customer data adequately and reasonably, treating the failure to employ
8 reasonable and appropriate measures to protect against unauthorized access to
9 confidential consumer data as an unfair act or practice prohibited by Section 5 of the
10 FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the
11 measures businesses must take to meet their data security obligations.

12 39. City of Hope failed to properly implement basic data security practices.
13 City of Hope's failure to employ reasonable and appropriate measures to protect
14 against unauthorized access to patients' Private Information constitutes an unfair act
15 or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

16 40. City of Hope was at all times fully aware of its obligation to protect its
17 patients' Private Information because of its position as a healthcare provider. City of
18 Hope was also aware of the significant repercussions that would result from its
19 failure to do so.

CLASS ALLEGATIONS

21 30. Plaintiff brings this case individually and, pursuant to Rule 23 of the
22 Federal Rules of Civil Procedure, on behalf of the following class:

23 All individuals in the United States whose Private
24 Information was compromised in the Defendant's Data
Breach disclosed on April 2, 2024.

25 31. Excluded from the Classes is Defendant, its subsidiaries and affiliates,
26 its officers, directors and members of their immediate families and any entity in
27 which Defendant has a controlling interest, the legal representative, heirs,

²¹ FTC, *Start With Security*, *supra*.

1 successors, or assigns of any such excluded party, the judicial officer(s) to whom
2 this action is assigned, and the members of their immediate families.

3 32. Plaintiff reserves the right to modify or amend the definition of the
4 proposed Class prior to moving for class certification.

5 41. **Numerosity:** The Class Members are so numerous that individual
6 joinder of all Class Members is impracticable. City of Hope has disclosed that the
7 Data Breach affected approximately 827,149 patients.

8 42. **Commonality:** There are questions of law and fact common to the
9 Class, which predominate over any questions affecting only individual Class
10 Members. These common questions of law and fact include, without limitation:

- 11 a. Whether and to what extent Defendant had a duty to protect the Private
12 Information of Class Members;
- 13 b. Whether Defendant was negligent in collecting and storing Plaintiff and
14 Class Members' Private Information;
- 15 c. Whether Defendant had duties not to disclose the Private Information
16 of Class Members to unauthorized third parties;
- 17 d. Whether Defendant took reasonable steps and measures to safeguard
18 Plaintiff and Class Members' Private Information;
- 19 e. Whether Defendant failed to adequately safeguard the Private
20 Information of Class Members;
- 21 f. Whether Defendant failed to implement and maintain reasonable
22 security policies and practices appropriate to the nature and scope of
23 the Private Information compromised in the Data Breach;
- 24 g. Whether Defendant adequately, promptly, and accurately informed
25 Plaintiff and Class Members that their Private Information had been
26 compromised;

- 1 h. Whether Plaintiff and Class Members are entitled to actual damages,
2 statutory damages, and/or punitive damages because of Defendant's
3 wrongful conduct;
- 4 i. Whether Plaintiff and Class Members are entitled to restitution because
5 of Defendant's wrongful conduct;
- 6 j. Whether Plaintiff and Class Members are entitled to injunctive relief to
7 redress the imminent and ongoing harm they face because of the Data
8 Breach; and
- 9 k. Whether Plaintiff and Class Members are entitled to identity theft
10 protection for their respective lifetimes.

11 43. **Typicality:** Plaintiff's claims are typical of those of other Class
12 Members because Plaintiff Private Information, like that of every other Class
13 Member, was disclosed by City of Hope. Plaintiff's claims are typical of those of the
14 other Class Members because, *inter alia*, all Class Members were injured through
15 Defendant's common misconduct. Plaintiff are advancing the same claims and legal
16 theories individually and on behalf of all other Class Members, and there are no
17 defenses that are unique to Plaintiff. Plaintiff claims and Class Members' claims
18 arise from the same operative facts and are based on the same legal theories.

19 44. **Adequacy:** Plaintiff is an adequate representatives of the Class because
20 Plaintiff are members of the Class and are committed to pursuing this matter against
21 City of Hope to obtain relief for the Class. Plaintiff has no conflicts of interest with
22 the Class. Plaintiff's counsel are competent and experienced in litigating class
23 actions, including extensive experience in data breach litigation. Plaintiff intends to
24 vigorously prosecute this case and will fairly and adequately protect the Class's
25 interests.

26 45. **Policies Generally Applicable to the Class:** This class action is also
27 appropriate for certification because City of Hope has acted or refused to act on
28 grounds generally applicable to the Class, thereby requiring the Court's imposition

1 of uniform relief to ensure compatible standards of conduct toward the Class
2 Members and making final injunctive relief appropriate with respect to the Class as
3 a whole. City of Hope's policies challenged herein apply to and affect Class
4 Members uniformly and Plaintiff's challenge of these policies hinges on City of
5 Hope's conduct with respect to the Class as a whole, not on facts or law applicable
6 only to Plaintiff.

7 **46. Superiority:** Class litigation is an appropriate method for fair and
8 efficient adjudication of the claims involved. Class action treatment is superior to all
9 other available methods for the fair and efficient adjudication of the controversy
10 alleged herein; it will permit a large number of Class Members to prosecute their
11 common claims in a single forum simultaneously, efficiently, and without the
12 unnecessary duplication of evidence, effort, and expense that hundreds of individual
13 actions would require. Class action treatment will permit the adjudication of
14 relatively modest claims by certain Class Members, who could not individually
15 afford to litigate a complex claim against large corporations, like City of Hope. Even
16 for those Class Members who could afford to litigate such a claim, it would still be
17 economically impractical and impose a burden on the courts.

18 **47.** The nature of this action and the nature of laws available to Plaintiff
19 and Class Members make the use of the class action device a particularly efficient
20 and appropriate procedure to afford relief to Plaintiff and Class Members for the
21 wrongs alleged because City of Hope would necessarily gain an unconscionable
22 advantage in non-class litigation, since City of Hope would be able to exploit and
23 overwhelm the limited resources of each individual Class Member with superior
24 financial and legal resources; the costs of individual suits could unreasonably
25 consume the amounts that would be recovered; proof of a common course of conduct
26 to which Plaintiff were exposed is representative of that experienced by Class
27 Members and will establish the right of each Class Member to recover on the causes
28

of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

48. The litigation of Plaintiff claims is manageable. City of Hope's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

49. Adequate notice can be given to Class Members directly using information maintained in City of Hope's records.

50. Unless a class-wide injunction is issued, City of Hope may continue to maintain inadequate security with respect to the Private Information of Class Members, City of Hope may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and City of Hope may continue to act unlawfully as set forth in this Complaint.

COUNT I

NEGLIGENCE

(on behalf of Plaintiff and the Class)

51. Plaintiff re-allege and incorporate by reference herein all the allegations contained in paragraphs 1-50.

52. City of Hope knowingly collected, came into possession of, and maintained Plaintiff and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing City of Hope's security protocols to ensure that Plaintiff and Class Members' Private Information in Defendant's possession was adequately secured and protected, that Plaintiff and Class Members' Private Information on City of Hope's networks were not accessible to criminals without authorization, and that City of Hope employees

1 tasked with maintaining such information were adequately trained on security
2 measures regarding the security of customers/patients' Private Information.

3 53. As a condition of utilizing City of Hope's services, Plaintiff and Class
4 Members were obligated to provide their Private Information to City of Hope.

5 54. Plaintiff and Class Members entrusted their Private Information to City
6 of Hope with the understanding that City of Hope would safeguard their information,
7 use their Private Information for business purposes only, and not disclose their
8 Private Information to unauthorized third parties.

9 55. City of Hope knew or reasonably should have known that a failure to
10 exercise due care in the collecting, storing, and using Plaintiff and Class Members'
11 Private Information involved an unreasonable risk of harm to Plaintiff and Class
12 Members.

13 56. City of Hope also had a duty to have procedures in place to detect and
14 prevent the improper access and misuse of Plaintiff and Class Members' Private
15 Information.

16 57. A breach of security, unauthorized access, and resulting injury to
17 Plaintiff and Class Members was reasonably foreseeable, particularly in light of prior
18 data breaches and disclosures prevalent in today's digital landscape, including the
19 explosion of data breaches involving similarly situated healthcare providers.

20 58. Plaintiff and Class Members were the foreseeable and probable victims
21 of any inadequate security practices and procedures. City of Hope knew or should
22 have known of the inherent risks in collecting and storing Plaintiff and Class
23 Members' Private Information, the critical importance of providing adequate
24 security of that information, the necessity for encrypting PHI stored on City of
25 Hope's systems, and that it had inadequate IT security protocols in place to secure
26 Plaintiff and Class Members' Private Information.

27 59. City of Hope's own conduct created a foreseeable risk of harm to
28 Plaintiff and Class Members. City of Hope's misconduct included, but was not

1 limited to, failure to take the steps and opportunities to prevent the Data Breach as
2 set forth herein.

3 60. Plaintiff and Class Members had no ability to protect their Private
4 Information that was in City of Hope's possession.

5 61. City of Hope was in a position to protect against the harm suffered by
6 Plaintiff and Class Members as a result of the Data Breach.

7 62. City of Hope had, and continues to have, a duty to timely disclose that
8 Plaintiff and Class Members' Private Information within its possession was
9 compromised and precisely the type(s) of information that were compromised.

10 63. City of Hope had a duty to have procedures in place to detect and
11 prevent the loss or unauthorized dissemination of Plaintiff and Class Members'
12 Private Information.

13 64. City of Hope systematically failed to provide adequate security for data
14 in its possession.

15 65. City of Hope, through its actions and/or omissions, unlawfully
16 breached its duty to Plaintiff and Class Members by failing to exercise reasonable
17 care in protecting and safeguarding Plaintiff and Class Members' Private
18 Information within its possession.

19 66. City of Hope, through its actions and/or omissions, unlawfully
20 breached its duty to Plaintiff and Class Members by failing to have appropriate
21 procedures in place to detect and prevent dissemination of Plaintiff and Class
22 Members' Private Information.

23 67. City of Hope, through its actions and/or omissions, unlawfully
24 breached its duty to timely disclose to Plaintiff and Class Members that the Private
25 Information within City of Hope's possession might have been compromised and
26 precisely the type of information compromised.

27 68. City of Hope breach of duties owed to Plaintiff and Class Members
28 caused Plaintiff and Class Members' Private Information to be compromised.

1 69. But for all of City of Hope's acts of negligence detailed above,
2 including allowing cyber criminals to access its systems containing Plaintiff and
3 Class Members' Private Information would not have been compromised.

4 70. Plaintiff never transmitted her own unencrypted PHI over the internet
5 or any other unsecured source.

6 71. Following the Data Breach, Plaintiff's PHI has been seized by
7 unauthorized third parties who are now free to exploit and misuse that PHI without
8 any ability for Plaintiff to recapture and erase that PHI from further dissemination—
9 Plaintiff's PHI is forever compromised.

10 72. But for the Data Breach, Plaintiff would not have incurred the loss and
11 publication of her PHI and other injuries.

12 73. There is a close causal connection between City of Hope's failure to
13 implement security measures to protect Plaintiff and Class Members' Private
14 Information and the harm suffered, or risk of imminent harm suffered by Plaintiff
15 and Class Members. Plaintiff and Class Members' PHI was accessed and
16 compromised as the proximate result of City of Hope's failure to exercise reasonable
17 care in safeguarding such Private Information by adopting, implementing, and
18 maintaining appropriate security measures and encryption.

19 74. Plaintiff and Class Members now face years of constant surveillance of
20 their financial and personal records, monitoring, loss of privacy, and loss of rights.
21 The Class is incurring and will continue to incur such damages in addition to any
22 fraudulent use of their Private Information.

23 75. As a result of City of Hope's negligence and breach of duties, Plaintiff
24 and Class Members are in danger of imminent harm in that their Private Information,
25 which is still in the possession of third parties, will be used for fraudulent purposes.

26 76. Plaintiff seeks the award of actual damages on behalf of themselves and
27 the Class.

77. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling City of Hope to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling City of Hope to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

COUNT II

NEGLIGENCE PER SE

(on behalf of Plaintiff and the Class)

78. Plaintiff re-allege and incorporate by reference herein all the allegations contained in paragraphs 1-50.

79. Pursuant to the HIPAA (42 U.S.C. § 1302d et seq.), the FTC Act, City of Hope was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff and Class Members' Private Information.

80. City of Hope breached its duties by failing to employ industry standard data and cybersecurity measures to ensure its compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

81. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to City of Hope networks, databases, and computers that stored or contained Plaintiff and Class Members' Private Information.

82. Plaintiff and Class Members' Private Information constitutes personal property that was stolen due to City of Hope's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

1 83. City of Hope's conduct in violation of applicable laws directly and
2 proximately caused the unauthorized access and disclosure of Plaintiff and Class
3 Members' unencrypted Private Information, and Plaintiff and Class Members have
4 suffered and will continue to suffer damages as a result of City of Hope's conduct.
5 Plaintiff and Class Members seek damages and other relief as a result of City of
6 Hope's negligence.

COUNT III

BREACH OF IMPLIED CONTRACT

(on behalf of Plaintiff and the Class)

10 84. Plaintiff re-allege and incorporate by reference herein all the allegations
11 contained in paragraphs 1-50.

12 85. When Plaintiff and Class Members provided their Private Information
13 to City of Hope they entered into implied contracts with City of Hope, under which
14 City of Hope agreed to take reasonable steps to protect Plaintiff and Class Members'
15 Private Information, comply with its statutory and common law duties to protect
16 Plaintiff and Class Members' Private Information, and to timely notify them in the
17 event of a data breach.

18 86. City of Hope solicited and invited Plaintiff and Class Members to
19 provide their Private Information as part of provision of healthcare services.
20 Plaintiff and Class Members accepted City of Hope's offers and provided their
21 Private Information to City of Hope.

22 87. When entering into implied contracts, Plaintiff and Class Members
23 reasonably believed and expected that City of Hope's data security practices
24 complied with its statutory and common law duties to adequately protect Plaintiff
25 and Class Members' Private Information and to timely notify them in the event of a
26 data breach.

27 88. Plaintiff and Class Members paid money to City of Hope to receive
28 healthcare services. Plaintiff and Class Members reasonably believed and expected

1 that City of Hope would use part of those funds to obtain adequate data security.

2 City of Hope failed to do so.

3 89. Plaintiff and Class Members would not have provided their Private
4 Information to City of Hope had they known that they would not safeguard their
5 Private Information, as promised, or provide timely notice of a data breach.

6 90. Plaintiff and Class Members fully performed their obligations under
7 their implied contracts with City of Hope.

8 91. City of Hope breached its implied contracts with Plaintiff and Class
9 Members by failing to safeguard Plaintiff and Class Members' Private Information
10 and by failing to provide them with timely and accurate notice of the Data Breach.

11 92. The losses and damages Plaintiff sustained, include, but are not limited
12 to:

- 13 a. Theft of their Private Information;
- 14 b. Costs associated with purchasing credit monitoring and identity theft
15 protection services;
- 16 c. Costs associated with the detection and prevention of identity theft and
17 unauthorized use of their Private Information;
- 18 d. Lowered credit scores resulting from credit inquiries following
19 fraudulent activities;
- 20 e. Costs associated with time spent and the loss of productivity from
21 taking time to address and attempt to ameliorate, mitigate, and deal with
22 the actual and future consequences of the Data Breach – including
23 finding fraudulent charges, cancelling, and reissuing cards, enrolling in
24 credit monitoring and identity theft protection services, freezing and
25 unfreezing accounts, and imposing withdrawal and purchase limits on
26 compromised accounts;

- 1 f. The imminent and certainly impending injury flowing from the
- 2 increased risk of potential fraud and identity theft posed by their Private
- 3 Information being placed in the hands of criminals;
- 4 g. Damages to and diminution in value of their Private Information
- 5 entrusted, directly or indirectly, to City of Hope with the mutual
- 6 understanding that City of Hope would safeguard Plaintiff and Class
- 7 Members' data against theft and not allow access and misuse of their
- 8 data by others;
- 9 h. Continued risk of exposure to hackers and thieves of their Private
- 10 Information, which remains in City of Hope's possession and is subject
- 11 to further breaches so long as City of Hope fails to undertake
- 12 appropriate and adequate measures to protect Plaintiff and Class
- 13 Members' data; and
- 14 i. Emotional distress from the unauthorized disclosure of Private
- 15 Information to strangers who likely have nefarious intentions and now
- 16 have prime opportunities to commit identity theft, fraud, and other
- 17 types of attacks on Plaintiff and Class Members.

18 93. As a direct and proximate result of City of Hope's breach of contract,
19 Plaintiff and Class Members are entitled to damages, including compensatory,
20 punitive, and/or nominal damages, in an amount to be proven at trial.

21 **COUNT IV**

22 **BREACH OF FIDUCIARY DUTY**

23 **(on behalf of Plaintiff and the Class)**

24 94. Plaintiff re-allege and incorporate by reference herein all the
25 allegations contained in paragraphs 1-50.

26 95. City of Hope has a fiduciary duty to act for the benefit of Plaintiff and
27 Class Members upon matters within the scope of their relationship, as a consequence

1 of the special relationship of trust and confidence that exists between patients (like
2 Plaintiff and Class Members) and their medical care providers (like City of Hope).

3 96. In light of their special relationship, City of Hope has become the
4 guardian of Plaintiff and Class Members' Private Information. City of Hope has
5 become a fiduciary, created by its undertaking and guardianship of patient Private
6 Information, to act primarily for the benefit of its patients, including Plaintiff and
7 Class Members. This duty included the obligation to safeguard Plaintiff and Class
8 Members' Private Information and to timely notify them in the event of a data
9 breach.

10 97. City of Hope breached its fiduciary duties owed to Plaintiff and Class
11 Members by failing to:

- 12 a. properly encrypt and otherwise protect the integrity of the system
13 containing Plaintiff and Class Members' Private Information;
- 14 b. timely notify and/or warn Plaintiff and Class Members of the Data
15 Breach;
- 16 c. ensure the confidentiality and integrity of electronic protected health
17 information Defendant created, received, maintained, and transmitted,
18 in violation of 45 C.F.R. § 164.306(a)(1);
- 19 d. implement technical policies and procedures to limit access to only
20 those persons or software programs that have been granted access rights
21 in violation of 45 C.F.R. § 164.312(a)(1);
- 22 e. implement policies and procedures to prevent, detect, contain, and
23 correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);
- 24 f. identify and respond to suspected or known security incidents; mitigate
25 to the extent practicable, harmful effects of security incidents that are
26 known to the covered entity in violation of 45 C.F.R. §
27 164.308(a)(6)(ii);

- 1 g. protect against any reasonably-anticipated threats or hazards to the
2 security or integrity of electronic protected health information in
3 violation of 45 C.F.R. § 164.306(a)(2);
4 h. protect against any reasonably anticipated uses or disclosures of
5 electronic protected health information that are not permitted under the
6 privacy rules regarding individually identifiable health information in
7 violation of 45 C.F.R. § 164.306(a)(3);
8 i. ensure its compliance with the HIPAA security standard rules by its
9 workforce in violation of 45 C.F.R. § 164.306(a)(94);
10 j. properly use and disclose PHI that is and remains accessible to
11 unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;
12 k. effectively train all members of its workforce (including independent
13 contractors) on the policies and procedures with respect to protected
14 health information as necessary and appropriate for the members of its
15 workforce to carry out their functions and to maintain security of
16 protected health information in violation of 45 C.F.R. § 164.530(b) and
17 45 C.F.R. § 164.308(a)(5);
18 l. design, implement, and enforce policies and procedures establishing
19 physical and administrative safeguards to reasonably safeguard
20 protected health information, in compliance with 45 C.F.R. §
21 164.530(c); and
22 m. otherwise failing to safeguard Plaintiff and Class Members' Private
23 Information.

24 98. As a direct and proximate result of Defendant's breaches of its fiduciary
25 duties, Plaintiff and Class Members have suffered and will suffer injury, including,
26 but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or
27 theft of their Private Information; (iii) out-of-pocket expenses associated with the
28 prevention, detection, and recovery from identity theft and/or unauthorized use of

1 their Private Information; (iv) lost opportunity costs associated with effort
2 attempting to mitigate the actual and future consequences of the Data Breach,
3 including, but not limited to, efforts spent researching how to prevent, detect,
4 contest, and recover from identity theft; (v) the continued risk to their Private
5 Information, which remains in Defendant's possession and is subject to further
6 unauthorized disclosures so long as Defendant fails to undertake appropriate and
7 adequate measures to protect patient Private Information in their continued
8 possession; and (vi) future costs in terms of time, effort, and money that will be
9 expended to prevent, detect, contest, and repair the impact of the Private Information
10 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff
11 and Class Members.

12 99. As a direct and proximate result of Defendant's breach of its fiduciary
13 duty, Plaintiff and Class Members have suffered and will continue to suffer injury
14 and/or harm.

COUNT V

BREACH OF CONFIDENCE

(on behalf of Plaintiff and the Class)

18 100. Plaintiff re-allege and incorporate by reference herein all the allegations
19 contained in paragraphs 1-50.

20 101. Plaintiff and Class Members have an interest, both equitable and legal,
21 in their Private Information that was conveyed to, collected by, and maintained by
22 City of Hope - and that was accessed or compromised in the Data Breach.

23 102. City of Hope was provided with and stored private and valuable PHI
24 related to Plaintiff and the Class, which it was required to maintain in confidence.

25 103. Plaintiff and the Class provided City of Hope with their personal and
26 confidential PHI under both the express and/or implied agreement of City of Hope
27 to limit the use and disclosure of such PHI.

1 104. City of Hope owed a duty to Plaintiff and Class Members to exercise
2 the utmost care in obtaining, retaining, securing, safeguarding, deleting, and
3 protecting their PHI in its possession from being compromised, lost, stolen, accessed
4 by, misused by, or disclosed to unauthorized persons.

5 105. City of Hope had an obligation to maintain the confidentiality of
6 Plaintiff and Class Members' PHI.

7 106. Plaintiff and Class Members have a privacy interest in their personal
8 medical matters, and City of Hope had a duty not to disclose confidential medical
9 information and records concerning its patients.

10 107. As a result of the parties' relationship, City of Hope had possession and
11 knowledge of confidential PHI and confidential medical records of Plaintiff and
12 Class Members.

13 108. Plaintiff's and Class Members' PHI is not generally known to the public
14 and is confidential by nature.

15 109. Plaintiff and Class Members did not consent to nor authorize City of
16 Hope to release or disclose their PHI to unknown criminal actors.

17 110. City of Hope breached the duties of confidence it owed to Plaintiff and
18 Class Members when Plaintiff and Class Members' PHI was disclosed to unknown
19 criminal hackers.

20 111. City of Hope breached its duties of confidence by failing to safeguard
21 Plaintiff and Class Members' PHI, including by, among other things: (a)
22 mismanaging its system and failing to identify reasonably foreseeable internal and
23 external risks to the security, confidentiality, and integrity of customer information
24 that resulted in the unauthorized access and compromise of Private Information; (b)
25 mishandling its data security by failing to assess the sufficiency of its safeguards in
26 place to control these risks; (c) failing to design and implement information
27 safeguards to control these risks; (d) failing to adequately test and monitor the
28 effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to

1 evaluate and adjust its information security program in light of the circumstances
2 alleged herein; (f) failing to detect the breach at the time it began or within a
3 reasonable time thereafter; (g) failing to follow its privacy policies and practices
4 published to its patients; (h) storing PHI and medical records/information in an
5 unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i)
6 making an unauthorized and unjustified disclosure and release of Plaintiff and Class
7 Members' PHI and medical records/information to a criminal third party.

8 112. But for City of Hope's wrongful breach of its duty of confidences owed
9 to Plaintiff and Class Members, their privacy, confidences, and PHI would not have
10 been compromised.

11 113. As a direct and proximate result of City of Hope's breach of Plaintiff
12 and Class Members' confidences, Plaintiff and Class Members have suffered
13 injuries, including:

- 14 a. Loss of their privacy and confidentiality in their PHI;
- 15 b. Theft of their Private Information;
- 16 c. Costs associated with the detection and prevention of identity theft and
17 unauthorized use of their Private Information;
- 18 d. Costs associated with purchasing credit monitoring and identity theft
19 protection services;
- 20 e. Lowered credit scores resulting from credit inquiries following
21 fraudulent activities;
- 22 f. Costs associated with time spent and the loss of productivity from
23 taking time to address and attempt to ameliorate, mitigate, and deal with
24 the actual and future consequences of the City of Hope Data Breach –
25 including finding fraudulent charges, cancelling and reissuing cards,
26 enrolling in credit monitoring and identity theft protection services,
27 freezing and unfreezing accounts, and imposing withdrawal and
28 purchase limits on compromised accounts;

- 1 g. The imminent and certainly impending injury flowing from the
- 2 increased risk of potential fraud and identity theft posed by their Private
- 3 Information being placed in the hands of criminals;
- 4 h. Damages to and diminution in value of their Private Information
- 5 entrusted, directly or indirectly, to City of Hope with the mutual
- 6 understanding that City of Hope would safeguard Plaintiff and Class
- 7 Members' data against theft and not allow access and misuse of their
- 8 data by others;
- 9 i. Continued risk of exposure to hackers and thieves of their Private
- 10 Information, which remains in City of Hope's possession and is subject
- 11 to further breaches so long as City of Hope fails to undertake
- 12 appropriate and adequate measures to protect Plaintiff and Class
- 13 Members' data;
- 14 j. Loss of personal time spent carefully reviewing statements from health
- 15 insurers and providers to check for charges for services not received, as
- 16 directed to do by City of Hope; and
- 17 j. Mental anguish accompanying the loss of confidences and disclosure
- 18 of their confidential and private PHI.

19 114. Additionally, City of Hope received payments from Plaintiff and Class
20 Members for services with the understanding that City of Hope would uphold its
21 responsibilities to maintain the confidences of Plaintiff and Class Members' private
22 medical information.

23 115. City of Hope breached the confidence of Plaintiff and Class Members
24 when it made an unauthorized release and disclosure of their confidential medical
25 information and/or PHI and, accordingly, it would be inequitable for City of Hope
26 to retain the benefit at Plaintiff's and Class Members' expense.

27 116. As a direct and proximate result of City of Hope's breach of its duty of
28 confidences, Plaintiff and Class Members are entitled to damages, including

1 compensatory, punitive, and/or nominal damages, and/or disgorgement or
2 restitution, in an amount to be proven at trial.

3 **COUNT VI**

4 **UNJUST ENRICHMENT**

5 **(on behalf of Plaintiff and the Class)**

6 117. Plaintiff re-allege and incorporate by reference herein all the allegations
7 contained in paragraphs 1- 50.

8 118. Plaintiff and Class Members have an interest, both equitable and legal,
9 in their Private Information that was conferred upon, collected by, and maintained
10 by City of Hope and that was stolen in the Data Breach.

11 119. City of Hope benefitted from the conferral upon it of Plaintiff and Class
12 Members' Private Information, and by its ability to retain and use that information.
13 City of Hope understood that it so benefitted.

14 120. City of Hope also understood and appreciated that Plaintiff and Class
15 Members' Private Information was private and confidential and that its value
16 depended upon City of Hope maintaining its privacy and confidentiality.

17 121. But for City of Hope's willingness and commitment to maintain its
18 privacy and confidentiality, that Private Information would not have been transferred
19 to and entrusted with City of Hope. Further, if City of Hope had disclosed that its
20 data security measures were inadequate, City of Hope would not have been
21 permitted to continue in operation by regulators and the healthcare marketplace.

22 122. As a result of City of Hope's wrongful conduct as alleged in this
23 Complaint (including, among other things, its failure to employ adequate data
24 security measures, its continued maintenance and use of Plaintiff and Class
25 Members' Private Information without having adequate data security measures, and
26 its other conduct facilitating the theft of that Private Information), City of Hope has
27 been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class
28 Members.

1 123. City of Hope's unjust enrichment is traceable to, and resulted directly
2 and proximately from, the conduct alleged herein, including the compilation and use
3 of Plaintiff and Class Members' sensitive Private Information, while at the same
4 time failing to maintain that information secure from intrusion and theft by hackers.

5 124. Under the common law doctrine of unjust enrichment, it is inequitable
6 for City of Hope to be permitted to retain the benefits it received, and is still
7 receiving, without justification, from the use of Plaintiff and Class Members' Private
8 Information in an unfair and unconscionable manner. City of Hope's retention of
9 such benefits under circumstances making it inequitable to do so constitutes unjust
10 enrichment.

11 125. The benefit conferred upon, received, and enjoyed by City of Hope was
12 not conferred officially or gratuitously, and it would be inequitable and unjust for
13 City of Hope to retain the benefit.

COUNT VII

INJUNCTIVE/DECLARATORY RELIEF

(on behalf of Plaintiff and the Class)

17 126. Plaintiff re-allege and incorporate by reference herein all the allegations
18 contained in paragraphs 1-50.

19 127. City of Hope owes a duty of care to Plaintiff and Class Members
20 requiring it to adequately secure Private Information.

128. City of Hope still stores Plaintiff and Class Members' Private
Information.

23 129. Since the Data Breach, City of Hope has announced no specific changes
24 to its data security infrastructure, processes, or procedures to fix the vulnerabilities
25 in its computer systems and/or security practices which permitted the Data Breach
26 to occur and, thereby, prevent similar incidents from occurring in the future.

27 130. City of Hope has not satisfied its legal duties to Plaintiff and Class
28 Members.

1 131. Actual harm has arisen in the wake of the Data Breach regarding City
2 of Hope's duties of care to provide security measures to Plaintiff and Class
3 Members. Further, Plaintiff and Class Members are at risk of additional or further
4 harm due to the exposure of their Private Information, and City of Hope's failure to
5 address the security failings that led to that exposure.

6 132. Plaintiff, therefore, seek a declaration: (a) that City of Hope existing
7 security measures do not comply with its duties of care to provide adequate security;
8 and (b) that to comply with its duties of care, City of Hope must implement and
9 maintain reasonable security measures, including, but not limited to, the following:

- 10 a. ordering that City of Hope engage third-party security auditors as well
11 as internal security personnel to conduct testing, including simulated
12 attacks, penetration tests, and audits on City of Hope's systems on a
13 periodic basis, and ordering City of Hope to promptly correct any
14 problems or issues detected by such third-party security auditors;
- 15 b. ordering that City of Hope engage third-party security auditors and
16 internal personnel to run automated security monitoring;
- 17 c. ordering that City of Hope audit, test, and train its security personnel
18 regarding any new or modified procedures;
- 19 d. ordering that City of Hope segment patient data by, among other things,
20 creating firewalls and access controls so that if one area of City of
21 Hope's system is compromised, hackers cannot gain access to other
22 portions of City of Hope systems;
- 23 e. ordering that City of Hope purge, delete, and destroy in a reasonably
24 secure manner patient data not necessary for its provision of services;
- 25 f. ordering that City of Hope conduct regular computer system scanning
26 and security checks;
- 27 g. ordering that City of Hope routinely and continually conduct internal
28 training and education to inform internal security personnel how to

1 identify and contain a breach when it occurs and what to do in response
2 to a breach; and

3 h. ordering City of Hope to meaningfully educate its current, former, and
4 prospective patients about the threats they face because of the loss of
5 their PHI to third parties, as well as the steps they must take to protect
6 themselves.

7 **PRAAYER FOR RELIEF**

8 WHEREFORE Plaintiff, individually and on behalf of all others similarly
9 situated, pray for relief as follows:

- 10 a. for an Order certifying the Class as defined herein, and appointing Plaintiff
11 and her counsel to represent the Class;
- 12 b. for equitable relief enjoining City of Hope - from engaging in the wrongful
13 conduct complained of herein pertaining to the misuse and/or disclosure of
14 Plaintiff and Class Members' Private Information, and from refusing to
15 issue prompt, complete, and accurate disclosures to Plaintiff and Class
16 Members;
- 17 c. for equitable relief compelling City of Hope to use appropriate cyber
18 security methods and policies with respect to Private Information
19 collection, storage, and protection, and to disclose with specificity to Class
20 Members the types of Private Information compromised;
- 21 d. for an award of damages, including actual, nominal, consequential,
22 enhanced compensatory, and punitive damages, as allowed by law in an
23 amount to be determined;
- 24 e. for an award of attorneys' fees, costs, and litigation expenses, as allowed
25 by law;
- 26 f. for prejudgment interest on all amounts awarded; and
- 27 g. such other and further relief as this Court may deem just and proper.

1 **DEMAND FOR JURY TRIAL**

2 Plaintiff hereby demand a trial by jury on all issues so triable.

3 Dated: April 9, 2024

Respectfully submitted,

4 */s/ Kristen Lake Cardoso*
5 Kristen Lake Cardoso (State Bar No. 338762)
6 **KOPELOWITZ OSTROW, P.A.**
7 One West Las Olas Blvd., Suite 500
8 Fort Lauderdale, FL 33301
9 Tel: (954) 525-4100
10 cardoso@kolawyers.com
11 ostrow@kolawyers.com

12 Billy Pearce Howard*
13 Amanda J. Allen, Esquire*
14 **THE CONSUMER PROTECTION FIRM,
15 PLLC**
16 401 East Jackson Street, Suite 2340
17 Truist Place
18 Tampa, FL 33602
19 Tel: (813) 500-1500
20 Billy@TheConsumerProtectionFirm.com
21 Amanda@TheConsumerProtectionFirm.com

22 *Attorneys for Plaintiff and the Putative Class*